REMARKS

Initially, in the Office Action dated May 17, 2004, the Examiner rejects claims 1-11, 13, 18 and 28-32 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,163,147 (Orita). Claim 12 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of WO 99/00958 (Leveridge et al.). Claims 14-17 and 20-26 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of BLUETOOTH: Visions, Goals, and Architecture (Haartsen et al.). Claims 19 and 27 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of U.S. Patent No. 5,818,936 (Mashayekhi).

Claims 1-32 remain pending in the present application.

35 U.S.C. §102 Rejections

Claims 1-11, 13, 18 and 28-32 have been rejected under 35 U.S.C. §102(b) as being anticipated by Orita. Applicants have discussed the deficiencies of Orita in Applicants previously-filed response and re-submit all remarks submitted in this response. Applicants respectfully traverse these rejections and provide the following additional remarks.

Regarding claims 1, 28, 31 and 32, Applicants submit that Orita does not disclose or suggest the limitations in the combination of each of these claims of, inter alia, access control means accessible by a communicating device requesting access to a first application without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access

control means instructs the authentication means to authenticate the communicating device, or arbitrating the access of a requesting device to a service provided to a providing device that includes determining, in an arbitration means, whether to grant or refuse access to a first application by the requesting device, wherein if the determination requires authentication of the requesting device, the authentication is performed during that determination and not previously, or arbitration means for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and arranged to receive from the interface an indication, originating from the other device, identifying the other device wherein if the requesting device has a stored trust indication associated therewith, no user authorization is required, and if the requesting device has no stored trust indication associated therewith, user authorization being required.

The examiner alleges that Orita discloses two authentications--that the first authentication (input of the user ID and password) is "a standard login that is well known in the art of networking" and that the second authentication is the input of "EP authenticating parameters in order to access the secure resources". The examiner considers that the first authentication is separate to the second authentication. Consequently, the examiner makes the conclusion that "the user can access a system first without having to prove that he\she has access to any particular network resources" and that "it is only when the user requests the resources must he\she provide the EP [password]".

Orita discloses that a user ID and password, input by a user into the work station 10, are searched against OP information, stored on a storage unit 12c. If they match one another, the user is recognized as a registered user and is allowed to log on to the system. At this stage, OP information is read out from the storage unit 12c and stored in area 14a of the host computer 11. One user program is stored in one EP information file and a user who is entitled to access the EP information file can open the user program stored in the EP information file. An EP password is entered by the user, along with the name of the EP information file, in order to check whether access to an EP information file is allowed or prohibited (see col. 3 lines 63 - 67). The EP password can be shared amongst many users (Col. 5, lines 56-59). Additionally, access to the EP information file is determined by an EP authority level which is compared with the authority level of the operator profile (see col. 3 line 67 to col. 4, line 8). The EP authority level appears to be an authority level that is associated with the EP information file which can be shared amongst many users. The EP authority level is not associated with the identity of the user. If the check is successful, the host computer 11 reads the EP information 12d, defined by the OP information 12c, out of the storage unit 12 and stores it in the host computer 11.

If a user has access to the EP information file on the host computer 11, he may activate a user program defined in the EP information file to access and modify files. In order to access a file, the user program checks whether a password stored in the EP information file corresponds to a password contained in access protection information 12a of the file to be accessed (see col. 4, line 52 to col. 5 line 37). The access protection information includes information on the password and access type

of a file and is contained within the file. In addition, the user program is allotted with an authority level, and access to the file by the user is prohibited if the user's authority level (as defined by the OP information) is lower than that of the user program. When a request to access a file is permitted, determination of permission of execution of access is made based on the access protection information (see col. 5, lines 30 to 34).

Therefore, Orita merely discloses that a file contains access protection information including a password and type of access. Access to a file depends on a password contained in the EP information file and the authority level of the user contained in the OP. Access to a program depends on the input EP password and the authority level of the user contained in the OP. Consequently, neither access to a file or a program requires user authentication at the point of access but does require user authentication at logon to obtain the OP. It is therefore essential that user authentication and obtaining OP information occurs before determining whether access to a file / program should be allowed.

The examiner is incorrect in his assessment of Orita. The examiner alleges that the input of user ID is independent of the input of an EP password to access user programs or files. As described on col. 3, line 53 to col. 4, line 9, the operator profile authority level is used in combination with the EP password to determine whether access to an EP information file is allowed and hence access to a user program. The operator profile is previously downloaded from the storage unit 14 to the host computer 11 in response to the input of a user ID and password that corresponds to an operator profile. Therefore, the Examiner has misinterpreted

Orita. Orita discloses that access to an EP information file is dependent upon the OP authority level which is provided by the authentication of the user. Moreover, as mentioned above, determination of access to a file is also made by comparing the authority level of the user (as defined by the operator profile) with the authority level of the program. Thus, access to a file is dependent upon the OP authority level.

Therefore, Orita does not disclose or suggest access control means accessible by a communicating device requesting access to the first application without the communicating device having been authenticated by the authentication means, as recited in the claims of the present application. In Orita, a user must always input their user ID and password and be authenticated by the computer system in order to obtain an OP and then access user programs or files.

Additionally, Orita teaches that the EP information may not be specific to an individual user, but generic to a group of users. In this case, the EP information would be incapable of identifying and authenticating a specific user. Therefore, even if we view Orita in line with the examiners assertion that the entering of an EP password is a separate authentication, the resultant computer system would not be able to authenticate a specific user. Consequently, the teaching of Orita is clear, the purpose of the input of the user ID and password is to first authenticate a user. The EP information, in combination with the OP information, is used to provide a level of security for user programs and files once the user has been authenticated.

The Examiner reasserts that Orita discloses access control means accessible by a communicating device requesting access to a first application without the communicating device having been authenticated by the authenticating means, . . .

as recited in the claims of the present application, in Orita at col. 1, lines 51-56 and col. 2, lines 10-19. However, as noted in Applicants' previously-filed response, these portions of Orita merely disclose a computer system having a security function capable of attaining the security according to the content of a file and the access type at the time of accessing file by a user so as to affect a reliable security operation for files, and that it is determined whether execution of file access is permitted or not based on the access protection information read out from a second storage unit when an access request is made with respect to a specified file stored in a first storage unit according to a user program. This is not a communicating device requesting access to a first application without the communicating device having been authenticated by an authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructing the authentication means to authenticate the communicating device, as recited in the claims of the present application. These portions of Orita do not disclose or suggest a communicating device requesting access to an application, or determining whether a communicating device has been authenticated by an authentication means. Further, these portions of Orita do not disclose or suggest an authentication means to authenticate a communicating device if arbitration requires an authentication of the communicating device. These portions of Orita merely disclose attaining security according to the content of a file where execution of file access is determined based on the access protection information

read out from a storage unit. The claims of the present application relate to access to an application. In contrast, Orita relates to access to a file.

Regarding claims 2-11, 13, 18 and 29, Applicants submits that these claims are dependent on one of independent claims 1 and 28 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. For example, Orita does not disclose or suggest the access control means being arranged to store security indications in association with accessible applications, wherein the stored security indication associated with the first application is indicative of whether authentication of the communicating device is or is not required during arbitration.

Accordingly, Applicants submit that Orita does not disclose or suggest the limitations in the combination of each of claims 1-11, 13, 18 and 28-32 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

35 U.S.C. §103 Rejections

Claim 12 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of Leveridge et al. Applicants respectfully traverse this rejection.

Applicants submit that claim 12 is dependent on independent claim 1 and, therefore, is patentable at least for the same reasons noted previously regarding this independent claim. Applicants submit that Leveridge et al. does not overcome the substantial defects noted previously regarding Orita. For example, none of the cited references disclose or suggest authentication comprising secret key exchange between the device and the communicating device.

Accordingly, Applicants submit that neither Orita nor Leveridge et al. taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of claim 12 of the present application. Applicants respectfully request that this rejection be withdrawn and that this claim be allowed.

Claims 14-17 and 20-26 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of Haartsen et al. Applicants respectfully traverse these rejections.

Applicants submit that claims 14-17 and 20-26 are dependent on independent claim 1 and, therefore, are patentable at least for the same reasons noted regarding this independent claim. Applicants submit that Haartsen et al. does not overcome the substantial defects noted previously regarding Orita. For example, Applicants submit that none of the cited references disclose or suggest each multiplexing protocol layer, in the route of the request as it proceeds up through the protocol stack, querying a security manager, which if the requested application is not connected to the querying protocol layer, allows access of the request through the querying protocol layer to a higher multiplexing protocol layer, and, if the requested application is connected to the querying protocol layer, performs an arbitration to grant or refuse access of the communicating device to the requested application.

Accordingly, Applicants submit that neither Orita nor Haartsen et al. taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 14-17 and 20-26 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 19 and 27 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Orita in view of Mashayekhi. Applicants have discussed the deficiencies of Mashayekhi in Applicants previously-filed response. The Examiner has failed to address Applicants' previous remarks in the outstanding Office Action. Applicants respectfully traverse these rejections.

Regarding claim 27, Applicants submit that neither Orita nor Mashayekhi, taken alone or in any proper combination, disclose or suggest the limitations in the combination of this claim of, inter alia, first access control means accessible by a communicating device requesting access to the first application program without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device, or second access control means accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the second application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device, wherein the first access control means is accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication means, and is arranged to provide the access of the

communicating device to the second access control means. As has been noted previously, Orita does not disclose or suggest these limitations in the claims of the present application. The Examiner admits that Orita fails to disclose or suggest a second access control means accessible by a communicating device requesting access to a second application . . . as recited in claim 27 of the present application, but asserts that Mashayekhi teaches these limitations at col. 5, lines 56-60 and col. 6, lines 43-59. However, these portions of Mashayekhi merely disclose that a workstation and server nodes may be configured as a distributed authentication service that automates an authentication exchange between a user interface, and that keychain objects associated with one or more application objects have attributes of at least one application secret and a public/private key pair where the application secret contains data used by a particular program to authenticate a user. Application secrets may be grouped according to access control level for each application program (e.g., requiring administrative rights for modification, allowing user modifications). This is not a second access control means accessible by a communicating device requesting access to a second application without the communicating device having been authenticated and the other associated limitations, as recited in the claims of the present application. These portions of Mashayekhi do not disclose or suggest anything related to arbitrating whether access of a communicating device is granted or refused or if arbitration requires authentication of a communicating device. Further, these portions of Mashayekhi do not disclose or suggest anything related to a first access control means being accessible by a communicating device requesting access to a second application

without the communicating device having been authenticated by an authentication means, and arranged to provide the access of the communicating device to the second access means, as recited in the claims of the present application. As noted, Mashayekhi discloses keychain objects associated with one or more application objects have attributes of at least one application secret and a public/private key pair where the application secret contains data used by a particular program to authenticate a user. The claims of the present application relate to authentication of a communicating device. In addition, Applicants do not interpret these portions of Mashayekhi the way the Examiner interprets it to indicate that once a user has been authenticated to system, the user can be authenticated to all of the other applications.

Regarding claim 19, Applicants submit that dependent on independent claim 1 and, therefore, is patentable at least for the same reasons noted regarding this independent claim. For example, Applicants submit that none of the cited references disclose or suggest the plurality of access control means being arranged in an hierarchy wherein a first access control means at the lowest level in the hierarchy provides access to at least a second access control means and access to one or both of a third access control means and an application, wherein access to each application is provided via one or more access control means including the first application control means and the application's connected access control means, if different, and wherein any access control means is accessible by a communicating device requesting access to one of its connected applications without the communicating device having been authenticated by the authentication means, and

being arranged to arbitrate whether access of the communicating device to the one connected application is granted or refused, the connected access control means instructing the authentication means to authenticate the communicating device if the arbitration requires an authentication of the communicating device.

Accordingly, Applicants submit that neither Orita nor Mashayekhi taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 19 and 27 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

In view of the foregoing amendments and remarks, Applicants submit that claims 1-32 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (referencing attorney docket no. 1156.41275X00).

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Frederick D. Bailey
Registration No. 42,282

FDB/sdb
(703) 312-6600